AO 91 (Rev. 11/11) Criminal Complaint (Rev. by USAO on 3/12/20) ☐ Original ☐ Duplicate Original

UNITED STATES DISTRICT COURT

for the

Central District of California

United States of America
v.
ROXANA ANDREA POPOVICI,

Defendant(s)

Case No. 2:25-MJ-03271-DUTY

CRIMINAL COMPLAINT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

As described in the accompanying attachment, defendant violated the following statutes:

Code Section	*Offense Description*
18 U.S.C. §§ 1344, 1349, 1028A; 8 U.S.C. § 1325(a)	Conspiracy to Commit Bank Fraud, Aggravated Identity Theft, Improper Entry by Alien

This criminal complaint is based on these facts:

Please see attached affidavit.

☒ Continued on the attached sheet.

/s Rene Persaud
Complainant's signature

Rene Persaud, Special Agent
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.

Date: May 29, 2025

Joel Richlin
Judge's signature

City and state: Los Angeles, California

Honorable A. Joel Richlin, U.S. Magistrate Judge
Printed name and title

AUSA Andrew Brown, 11th Floor, x0102

Complaint Attachment

Count One, 18 U.S.C. § 1349

Beginning in or before 2023, and continuing through May, 2025, in Los Angeles County, within the Central District of California, and elsewhere, defendant ROXANA ANDREA POPOVICI ("Defendant"), and others, conspired to commit bank fraud, in violation of Title 18, United States Code, Section 1344. The object of the conspiracy was carried out, and to be carried out, in substance, as follows: Defendant and her co-conspirators would secretly install skimming devices in ATMs to record the account information of bank customers, and would then counterfeit debit and credit cards bearing that information. Defendant and her co-conspirators would use the counterfeit cards to withdraw funds in the names of those victims of identity theft. Federally-insured financial institutions defrauded as a result of this conspiracy include Bank of America and US Bank.

Count Two, 18 U.S.C. § 1028A

Beginning in or before 2023, and continuing through May, 2025, in Los Angeles County, within the Central District of California, and elsewhere, defendant ROXANA ANDREA POPOVICI knowingly transferred, possessed, and used, without lawful authority, a means of identification of another person during and in relation to a felony violation of Title 18, United States Code, Section 1349, Conspiracy to Commit Bank Fraud, as charged in Count One, knowing that the means of identification belonged to another actual person.

Count Three, 8 U.S.C. § 1325(a)

On or about December 1, 2024, defendant ROXANA ANDREA POPOVICI, an alien who was not a natural-born or naturalized citizen, or national, of the United States, was found in Los Angeles County, within the Central District of California, after knowingly and voluntarily entering the United States from a foreign country either at a time and place other than as designated by immigration officers, or by a willfully false representation of a material fact.

AFFIDAVIT

I, Rene Persaud being duly sworn, declare and state as follows:

INTRODUCTION

1. I am a Special Agent ("SA") with the Federal Bureau of Investigation ("FBI"), and have been so employed since September 2018. Prior to becoming a SA, I worked for the FBI's Special Surveillance Group for approximately four years. Prior to joining the FBI, I was a Deputy Sheriff for the Hillsborough County (Florida) Sheriff's Office for approximately three years.

2. I have participated in various aspects of criminal enterprise investigations, including but not limited to, conducting surveillance and arrests, issuing subpoenas, seizing and impounding drug evidence, social media analysis, and the analysis of telephone tolls and other data. Additionally, I have interviewed and/or debriefed confidential informants and other witnesses who have had knowledge regarding the investigations in which I have been involved. I have also authored, sworn out, and executed multiple search warrants for various entities, including but not limited to, internet service providers, social media companies, GPS tracking units, and physical residences/businesses.

3. I also have extensive experience investigating Romanian Organized Criminal Groups. I have conducted investigations in the Los Angeles area related to the ATM skimming activity and money laundering, and I have also traveled to Romania on multiple occasions to work with National Police forces in several cities in order to obtain information, coordinate investigations, and identify criminals

who travel from Europe to the United States to defraud the American banking system.

PURPOSE OF AFFIDAVIT: COMPLAINT and SEARCH WARRANT

4. This affidavit is made in support of a complaint against ROXANA ANDREA POPOVICI for conspiracy to commit bank fraud, and aggravated identity theft, in violation of Title 18, United States Code, Sections 1344, 1349, and 1028A, and improper entry by an alien, in violation of Title 8, United States Code, Section 1325(a).

5. This affidavit is also made in support of search warrants for the residence and vehicle of POPOVICI for evidence of bank fraud, identity document fraud, money laundering, conspiracy to commit the same, and aggravated identity theft, in violation of Title 18, United States Code, Sections 1344, 1349, 1956, and 1028A, as described in Attachment B, which is incorporated by reference.

6. The information set forth in this affidavit is based upon my participation in the investigation, encompassing my personal knowledge, observations and experience, as well as information obtained through my review of evidence, investigative reports, and information provided by others, including other law enforcement partners. As this affidavit is being submitted for the limited purpose of securing the requested warrants, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause for the requested warrants.

PREMISES TO BE SEARCHED

7. The premises to be searched is:

a. 5659 WEST 8TH STREET APARTMENT 213, LOS ANGELES, CA (the "SUBJECT PREMISES"), described more fully in attachment A, which is incorporated by reference.

STATEMENT OF PROBABLE CAUSE

Summary:

8. The Federal Bureau of Investigation has been investigating a Romanian Organized Crime Group (OCG) operating in the United States involved in ATM skimming. As part of this investigation, the FBI identified ROXANA ANDREA POPOVICI as an individual involved in ATM skimming activity in and around Los Angeles. POPOVICI was captured on ATM video surveillance making unauthorized cash withdrawals from victim customer accounts in December 2024 and January 2025. In a four-day span, she illegally withdrew over $77,000 from victim customer accounts.

9. Additional investigation uncovered financial records indicating POPOVICI, who resides in the United States illegally and is not legally permitted to work, made over $77,000 in cash deposits between June 2024 and February 2025 in a single account. The Honorable Alicia G. Rosenberg issued a search warrant to track POPOVICI's cellular phone, and obtain historical location data, on May 20, 2025. Based on the data obtained from this warrant, as well as from physical surveillance, POPOVICI has been residing at the SUBJECT PREMISES since at least May 14, 2025.

Regulatory Background of CalFresh and CalWORKs Programs:

10. The California Department of Social Services (DSS) is a government agency that administers several benefit and assistance programs for residents of the state of California. One of the assistance programs administered by DSS is called CalFresh (formerly

known as food stamps), which helps low-income households purchase food and household items to meet their nutritional needs. Another assistance program administered by DSS is called CalWORKs, which helps low-income families with children pay for housing, food, and other necessary expenses.

11. Residents of California that meet the criteria established by the CalFresh or CalWORKs programs can apply online for benefits at www.getcalfresh.org and www.benefitscal.com. Beneficiaries apply for benefits by submitting their income and number of dependents to determine their benefit eligibility.

12. CalFresh and CalWORKs benefits are issued through Electronic Benefit Transfer cards ("EBT cards"). EBT cards are mailed to an address designated by the account holder and function like traditional debit cards to conduct transactions. For example, you can use an EBT card to make a purchase at a grocery or convenient store by swiping the card at a point-of-sale terminal.

13. The EBT cards issued under CalFresh and CalWORKs are assigned specific Bank Identification Numbers ("BIN"). A BIN refers to the first five digits of the account number on a debit or credit card and can be used to identify the issuer of the card, like DSS, which administers the CalFresh and CalWORKs programs.

14. Benefits received through the program are typically disbursed to EBT cardholders by DSS during the early days of each month. Those benefits are deposited directly from DSS into the account of the EBT cardholder.

15. The EBT cardholders can then conduct cash withdrawals at automated teller machines ("ATMs") using a personal identification

number ("PIN") established by the card holder. The EBT cardholder presents the card at an ATM, inserts the card into the ATM card reader, and utilizes a PIN to withdraw the funds previously deposited by DSS intended for beneficiaries of the CalFresh or CalWORKs programs.

Background on ATM Skimming and Access Device Fraud:

16. Based on my training and experience in investigating fraudulent schemes of this nature, I know the following about Access Device Fraud: ATM skimming devices are manually installed at walk-up or drive-thru ATM terminals. The card readers are surreptitiously inserted into the ATM card reader slots, and are often thin enough to go unnoticed to a lay person using an ATM. In addition to the card reader, another device is installed to obtain the PIN number. This device is often a covert camera that captures customers entering their PIN number.

17. An ATM skimming device is installed for a period of time after which the subjects who installed the device will return to the ATM and remove it. Once the device is removed, the customer credit card numbers and PIN numbers are retrieved from the device. The card numbers are then loaded on to blank cards so the perpetrators can travel to ATMs and fraudulently withdraw funds from victim customer accounts.

18. In addition to ATM skimmers, there are also devices known as Point-of-Sale skimmers. These devices are built to mimic the Point-of-Sale terminals at commercial businesses such as pharmacies, grocery stores, gas stations, and department stores. Because of the near identical design, these devices are installed by simply snapping

them on top of legitimate Point-of-Sale terminals in order to steal customer data when they complete their purchases at the above listed establishments. The data from these Point-of-Sale skimmers can be retrieved by recovering the device and downloading the data, or by downloading via Bluetooth when in close proximity to the device.

19. Based on my training and experience, I believe that members of the conspiracy I am investigating used the skimming techniques described above to capture the EBT card data of unsuspecting consumers. Historically, EBT cards have been issued by Bank of America. In my training and experience, all of the banks mentioned in this affidavit are federally insured.

POPOVICI Conducts Cash Outs from Victim EBT Cards:

20. In May 2025, the United States Secret Service informed me that they obtained data from DSS and US Bank about a woman who made consecutive cash withdrawals using stolen EBT cards at a US Bank branch ATM located at 11661 San Vicente Boulevard, Los Angeles, CA. These withdrawals took place on December 1-2, 2024, and January 1-2, 2025. US Bank provided images of the woman making these cash withdrawals, and they started precisely at 6:00 AM. I know from my training and experience that cash is deposited to EBT cards at 6:00 AM on the early days of the month. Professional ATM skimmers are aware of this fact and will begin their unauthorized cash withdrawals on or about 6:00 AM in an effort to steal funds before legitimate EBT customers can access them.

21. Based on DSS logs and US Bank transaction data of EBT cards used during this incident, which I reviewed, approximately $77,580

were stolen from 106 unique EBT cards during this four-day span. This resulted in an average loss of approximately $731 per card.

22. I reviewed the images of the woman who conducted these unauthorized cash withdrawals and compared them to a photo of POPOVICI during an attempted border crossing in April 2023. Based on this comparison, I was able to confirm that POPOVICI was the woman conducting the unauthorized cash withdrawals in these images on December 1-2, 2024 and January 1-2, 2025.

POPOVICI has Financial Activity Consistent with Skimmers:

23. POPOVICI is the owner of a Bank of America checking account (in her true name) that she opened in May 2023. This account, which lists the phone number 310-467-4065 ("Subject Telephone") as the contact number, has transactions that are consistent with the activity of Romanian ATM skimmers. POPOVICI, who resides in the United States illegally without the legal ability to work, made cash deposits between June 2024 and February 2025 of over $77,000. While criminals typically prefer to keep their illegal proceeds in cash to avoid tracing, in my training and experience they often deposit some of their stolen cash into an account which they can use to pay the kind of expenses that are not ordinarily transacted in cash, such as rent or international or wire transfers.

24. POPOVICI's bank account was used to transfer over $33,000 in outgoing wire transfers via Remitly (an international wire transfer service) between February 2024 and June 2025, and $6,750 in expenses at a plastic surgery clinic in February 2024. In addition, POPOVICI made 63 separate payments to the jail commissary accounts of an unknown number of inmates and detention facilities. These charges

indicate POPOVICI may be simultaneously laundering proceeds abroad, funding personal surgical enhancements with stolen EBT funds, and placing funds in the jail accounts of unknown co-conspirators.

POPOVICI Resides at the SUBJECT PREMISES:

25. As stated above, POPOVICI's bank account with her true name and personal information lists the Subject Telephone as her phone number. In addition, on May 20, 2025, I opened the application "WhatsApp" and searched for the Subject Telephone to see if there was a profile picture associated with the account. I found a WhatsApp account associated with the Subject Telephone and the profile picture clearly depicted POPOVICI's face. I know this to be POPOVICI's face because I was able to compare the photo taken during her attempted border crossing in April 2023 in her true name to the WhatsApp profile picture. Based on this comparison, I confirmed POPOVICI's photo was on the WhatsApp account associated with the Subject Telephone.

26. Based on these facts, the Honorable Alicia G. Rosenberg issued a phone tracker warrant for the Subject Telephone on May 2, 2025, which also authorized historical location data. Based on my review of this data, the Subject Telephone has consistently remained in the vicinity of the SUBJECT PREMISES during overnight hours since May 14, 2025 to May 28, 2025. Additionally, physical surveillance was conducted at the SUBJECT PREMISES on May 28, 2025. While standing in the hallway outside the SUBJECT PREMISES, I called the Subject Telephone to determine if the phone could be heard ringing inside. I did not hear an audible ringtone, but a woman with a European accent answered the phone. The woman said "hello, hello……who is this

motherf*cker." As this woman spoke, I could also clearly hear her voice from the hallway outside the SUBJECT PREMISES. Based on the fact I previously established that the Subject Phone belongs to POPOVICI, I believe that the woman I overheard speaking inside the SUBJECT PREMISES was in fact POPOVICI.

POPOVICI Resides in the US Illegally:

27. POPOVICI is currently residing in the United States illegally, and there is no record of her passing through a port of entry to the United States. On April 14, 2023, POPOVICI arrived on foot at a US/Canada land border in New York and applied for admission to enter the United States. She was refused entry and not allowed to enter the United States. On May 11, 2023, POPOVICI again arrived on foot at a US/Canada land border, this time in Montana, and applied for admission to enter the United States. She was refused entry again and not allowed to enter the United States. POPOVICI eventually made her way to the United States by unknown means and opened her bank account on May 31, 2023 in Los Angeles, CA. Based on my discussions with ICE agents, I know that if POPOVICI had lawfully entered the US using her true name at an authorized point of entry, there would be a record of her entering the US, and there is none. According to ICE-ERO, POPOVICI is amenable to removal from the United States. In my training and experience, members of Romanian ATM skimming crews commonly fly to either Canada and Mexico, where they do not face visa restrictions like they do for the US, and then illegally cross the land border into the US, usually by employing the services of professional alien smugglers.

Training and Experience Regarding Identity Theft and ATM Skimming

28. From my training and experience, and from discussions with other government officials, I know the following:

a. Members of ATM skimming crews maintain specialized equipment including skimmers, thin metal tools (often custom fabricated) to aid in the surreptitious insertion and removal of the skimmers, spy cameras to record PINs entered by customers, and magnetic strip reader-writers for counterfeiting ATM cards. Often times they possess plastic or metal housings designed to camouflage the spy cameras and make them blend in with the ATM. Often they have these custom made at plastic- or metal-working shops. Typically they have a stock of blank magnetic-strip cards, sometimes repurposed from gift cards, onto which they can write their stolen account information. The crew members usually write the PIN codes for the cards directly onto the counterfeits they produce.

b. Members of transnational ATM skimming crews typically enter the country either legally with a visa, if they have no criminal record and can pose as a legitimate tourist or business person, or through established immigrant-smuggling rings in Mexico and Canada otherwise. Oftentimes the crew members maintain false identity documents, which they use if arrested to make it harder to identify them. Some maintain false passports so that they can abscond if granted bail and flee the country.

c. Members of transnational ATM skimming crews have various ways of handling the proceeds of their offenses. Some is kept in cash for routine expenses. Some is usually deposited into a local bank account to pay for items for which cash would raise suspicion, such as rental cars and housing. The bulk, however, is

sent abroad either to their co-conspirators or home countries. This may be as simple as sending cash hidden among other items abroad through carriers such as DHL, or transfers through banks, Hawalas, Western Union, or similar services. More recently, the trend has been to purchase cryptocurrencies for cash.

d. Individuals involved in identity theft schemes like this one must keep evidence of their schemes, such as contact information for their co-conspirators, lists of victim information and accounts used in the scheme, simply to keep the scheme going. Much of this evidence is now stored on digital devices such as computers and smartphones.

e. Generally, perpetrators of skimming and identity theft schemes maintain this evidence where is close at hand and safe, such as in their residences, automobiles, and, especially with smartphones, on their person. For larger or more sophisticated frauds, participants often attempt to distance themselves from some of the incriminating evidence by renting public storage units or safety deposit boxes where they often keep the items they will not need immediate access to.

f. I have heard of cases in which card skimmers have embossed their own names on the front of counterfeit access devices so that they could use the counterfeit cards openly and with their own identification cards. I know from my training and experience that card skimmers and counterfeiters often re-encode gift cards that have no value left on them as credit or debit cards. This is both convenient for them as they can get their counterfeit stock for free and it makes the cards appear legitimate without elaborate additional

printing on them of logos and the like; the counterfeit credit and debit cards simply appear to be a gift card from a store. Both these techniques will likely prevent law enforcement from being able to tell if the facially legitimate looking cards are actually part of the skimming scheme just from seeing at them.

g. Members of a criminal conspiracy must of necessity communicate with one another. Commonly this is done by text, VOIP, email, telephone, or specialty communication application, often an encrypted one such as WhatsApp, and most often by smartphone. Members of the conspiracy commonly carry their smartphones, which include the contact information for their co-conspirators, on or near their persons, such as in their cars or residences.

TRAINING AND EXPERIENCE ON DIGITAL DEVICES[1]

29. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that the following electronic evidence, inter alia, is often retrievable from digital devices:

a. Forensic methods may uncover electronic files or remnants of such files months or even years after the files have been downloaded, deleted, or viewed via the Internet. Normally, when a person deletes a file on a computer, the data contained in the file does not disappear; rather, the data remain on the hard drive until

---

[1] As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as paging devices, mobile telephones, and smart phones; digital cameras; gaming consoles; peripheral input/output devices, such as keyboards, printers, scanners, monitors, and drives; related communications devices, such as modems, routers, cables, and connections; storage media; and security devices.

overwritten by new data, which may only occur after a long period of time. Similarly, files viewed on the Internet are often automatically downloaded into a temporary directory or cache that are only overwritten as they are replaced with more recently downloaded or viewed content and may also be recoverable months or years later.

b. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as, how the device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the form of configuration data stored by browser, e-mail, and chat programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

c. The absence of data on a digital device may be evidence of how the device was used, what it was used for, and who used it. For example, showing the absence of certain software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.

d. Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading filenames and extensions. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously

followed. Law enforcement continuously develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.

30. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it is not always possible to search devices for data during a search of the premises for a number of reasons, including the following:

a. Digital data are particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a complete and accurate analysis of data on digital devices, which may take substantial time, particularly as to the categories of electronic evidence referenced above. Also, there are now so many types of digital devices and programs that it is difficult to bring to a search site all of the specialized manuals, equipment, and personnel that may be required.

b. Digital devices capable of storing multiple gigabytes are now commonplace. As an example of the amount of data this equates to, one gigabyte can store close to 19,000 average file size (300kb) Word documents, or 614 photos with an average size of 1.5MB.

31. The search warrant requests authorization to use the biometric unlock features of a device, based on the following, which I know from my training, experience, and review of publicly available materials:

a. Users may enable a biometric unlock function on some digital devices. To use this function, a user generally displays a physical feature, such as a fingerprint, face, or eye, and the device will automatically unlock if that physical feature matches one the user has stored on the device. To unlock a device enabled with a fingerprint unlock function, a user places one or more of the user's fingers on a device's fingerprint scanner for approximately one second. To unlock a device enabled with a facial, retina, or iris recognition function, the user holds the device in front of the user's face with the user's eyes open for approximately one second.

b. In some circumstances, a biometric unlock function will not unlock a device even if enabled, such as when a device has been restarted or inactive, has not been unlocked for a certain period of time (often 48 hours or less), or after a certain number of unsuccessful unlock attempts. Thus, the opportunity to use a biometric unlock function even on an enabled device may exist for only a short time. I do not know the passcodes of the devices likely to be found in the search.

c. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose physical characteristics are among those that will unlock the device via biometric features, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be

possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, if while executing the warrant, law enforcement personnel encounter a digital device within the scope of the warrant that may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel to, with respect to ROXANA ANDREA POPOVICI and every other adult who is located at the SUBJECT PREMISES during the execution of the search who is reasonably believed by law enforcement to be a user of a biometric sensor-enabled device that falls within the scope of the warrant: (1) depress the person's thumb- and/or fingers on the device(s); and (2) hold the device(s) in front of the face of the person with his or her eyes open to activate the facial-, iris-, and/or retina-recognition feature.

d. In my training and experience, transnational ATM skimmer crews often reside together to better coordinate their efforts. This is especially true for persons involved in installing ATM skimming devices, and producing counterfeit cards, which requires specialized tools and equipment. One of the last search warrants I executed on such a residence yielded a skimming lab that covered the dining room table; the residence housed four different crew members, all of whom pled guilty to a federal felony. I have not seen a skimming operation in which non-criminal participants were also present. Indeed, it would be foolhardy to have non-criminal participants present at such a lab, as the illegal conduct would be

visible to them, and they might inform the authorities or otherwise compromise the secrecy the crew members require.

32. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

CONCLUSION

33. Based upon the foregoing facts and my training and experience, I believe there is probable cause to believe that POPOVICI conspired to commit bank fraud and committed aggravated identity theft and improper entry by an alien, and that evidence of the violations listed in Attachment B will be found at the SUBJECT PREMISES.

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this 29th day of May, 2025.

HON. A. JOEL RICHLIN
UNITED STATES MAGISTRATE JUDGE